RECONNAÎTRE LE HAMEÇONNAGE

Première vérification

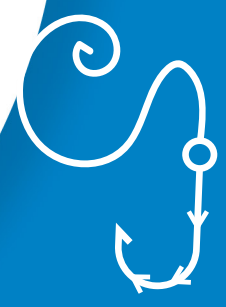
Les e-mails de phishing vous demanderont toujours quelque chose, parfois pour une raison apparemment tout à fait légitime. Soyez particulièrement vigilent si c'est soi-disant "très urgent". Vérifiez toujours si l'adresse e-mail et le nom de domaine utilisés correspondent bien à ceux de votre contact et si les liens renvoient bien à l'emplacement correct en maintenant votre souris dessus pendant un court instant. **Ne cliquez pas sur ces liens!**

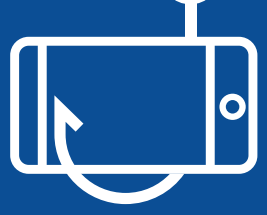
Hameçonnage ?

Cybercriminalité dans laquelle un attaquant se fait passer pour une source fiable afin d'obtenir des informations sensibles d'une victime.

Typosquattage ? Plutôt rusé !

Le typosquattage consiste à utiliser des noms de domaine mal orthographiés pour faire croire aux utilisateurs que le site qu'ils essaient de visiter est légitime. Si vous avez un doute, surfez vous-même sur le site web en question.





K Force Computer Solutions

YOUR PARTNER IN CLOUD, IT & TELECOM

Des doutes ? Contactez K Force !

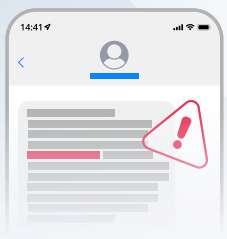
Helpdesk	**helpdesk@k-force.be**
Sales	**sales@k-force.be**
Proximus	**proximus@k-force.be**
Général	**info@k-force.be**
Administration	**administration@k-force.be**
Téléphone	**02 380 23 32**
Lu - ve	8h - 12h & 13h - 17h

Ne donnez jamais votre mot de passe ni des informations sensibles à des tiers !

Portez une attention particulière à l'hameçonnage ciblé

L'attaquant recherche les informations personnelles d'une cible spécifique, comme le nom de son employeur (et donc de ses collègues), des achats effectués en ligne récemment, etc... Avec ces données, l'attaquant peut envoyer un message d'apparence authentique semblant provenir d'une source fiable, telle que l'employeur, un collègue ou encore un fournisseur chez qui vous avez récemment commandé. Vous recevez soudain un e-mail étrange d'un collègue ? Attention !

Vishing et smishing



Il arrive aussi fréquemment que l'on tente d'accéder à vos données par téléphone (= vishing) ou par SMS (= smishing). Ne transmettez donc jamais de mot de passe via ces canaux, ne cliquez pas sur des liens suspects et évitez de communiquer des informations sensibles.

Vous avez reçu un message suspect ?

suspect@safeonweb.be

Formation et simulations axées sur la sensibilisation à la sécurité

www.k-force.be/fr/phishing